Preparing for the Cyber Battleground of the Future

2nd Lt Chris Babcock, USAF

Disclaimer: The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

For space and cyber Airmen, tomorrow's fight will be determined largely by the concept of cyberspace dependency. That term, as defined by the author, is the degree to which a military capability relies on supremacy over a portion of the cyberspace domain in order to cause or carry out its effects.[1] Cyber dependency is rapidly growing due to the cyberspace domain's exponential nature, the trajectory of market forces in the civilian world, and the strategic integration by the military of computer technology in the land, maritime, and air domains.[2]

Unlike employment in the three traditional war-fighting domains, the present employment of capabilities in the space domain *cannot* be achieved without cyberspace.[3] The recognition of this unique relationship between space and cyberspace has profound implications for recruitment; initial, intermediate, and advanced training; and development in the space and cyber career fields. A transition from the current force-development system towards one that acknowledges the unique relationship between space and cyberspace will have the additional benefit of informing the greater operational community as war fighters in the land, maritime, and air domains continue to become increasingly dependent upon cyberspace and space. This article discusses the implications of cyber dependency and proposes six recommendations to ensure that from recruitment to advanced training, space and cyber Airmen are prepared to excel in their interconnected domains.

Space Cyber Dependency

> *The relationship between space and cyberspace is unique in that virtually all space operations depend on cyberspace, and a critical portion of cyberspace can only be provided via space operations.*
>
> —Joint Publication 3-12 (R),
> *Cyberspace Operations*, 5 February 2013

All space operations currently performed by the US military are cyberspace dependent (fig. 1).[4] Space operations take place in the physical space domain, not within cyberspace. But because those who perform space operations are not physically present in space, they must rely entirely on control of their segment of cyberspace to transmit their commands to space vehicles in order to carry out space operations.[5]

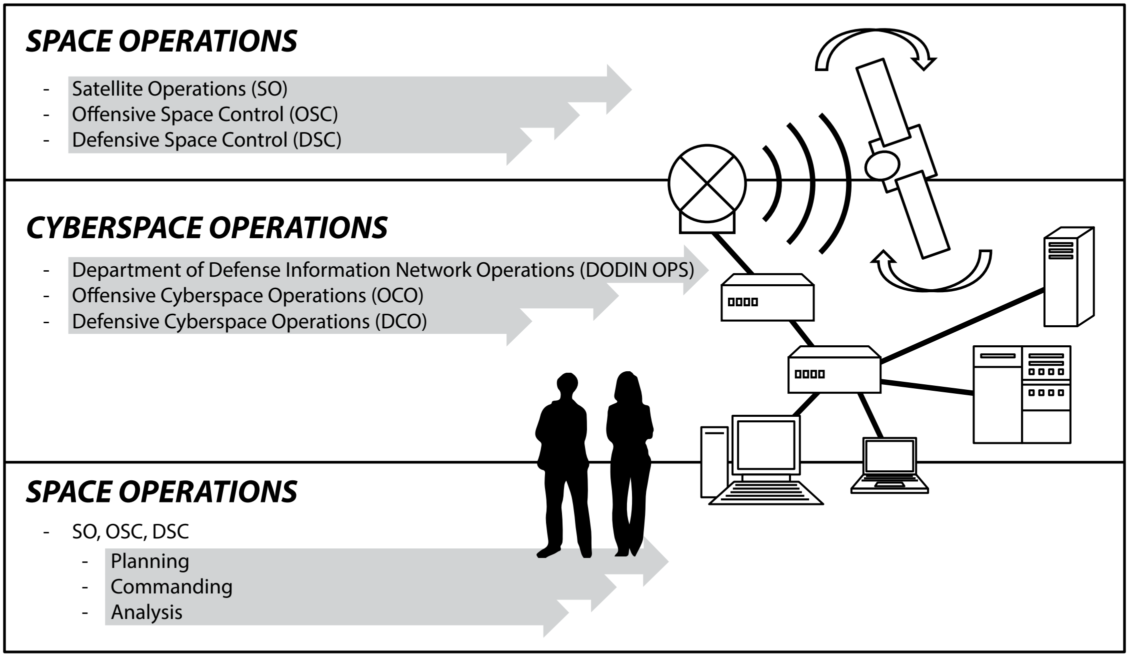
SPACE OPERATIONS
- Satellite Operations (SO)
- Offensive Space Control (OSC)
- Defensive Space Control (DSC)
CYBERSPACE OPERATIONS
- Department of Defense Information Network Operations (DODIN OPS)
- Offensive Cyberspace Operations (OCO)
- Defensive Cyberspace Operations (DCO)
SPACE OPERATIONS
- SO, OSC, DSC
- Planning
- Commanding
- Analysis

Figure 1. Space and cyberspace operations. Due to physical limitations, space operations take place on both sides of the cyberspace domain.

If a military space operation were to involve a pilot physically residing in a space vehicle, reacting to the environment in order to carry out effects in space, this would describe a space operation that is not reliant entirely on cyberspace supremacy.[6] In the absence of that scenario, space operators must use specialized computers and computer programs to transmit information to and from their space vehicles—which are themselves complex information systems—over a computer network.[7] Space's cyber dependency demands that special attention be paid to the cyber defense of space capabilities, but it also foreshadows the future state of the traditional war-fighting domains.

The physical network layer of cyberspace includes the information systems with which space operators command their satellites, the circuits connecting those information systems to the ground equipment, and the ground equipment itself. The logical network layer of cyberspace is embedded in each piece of the physical network. The cyber-persona layer describes the space operators who rely on the physical and logical network layers to perform space operations (fig. 2).

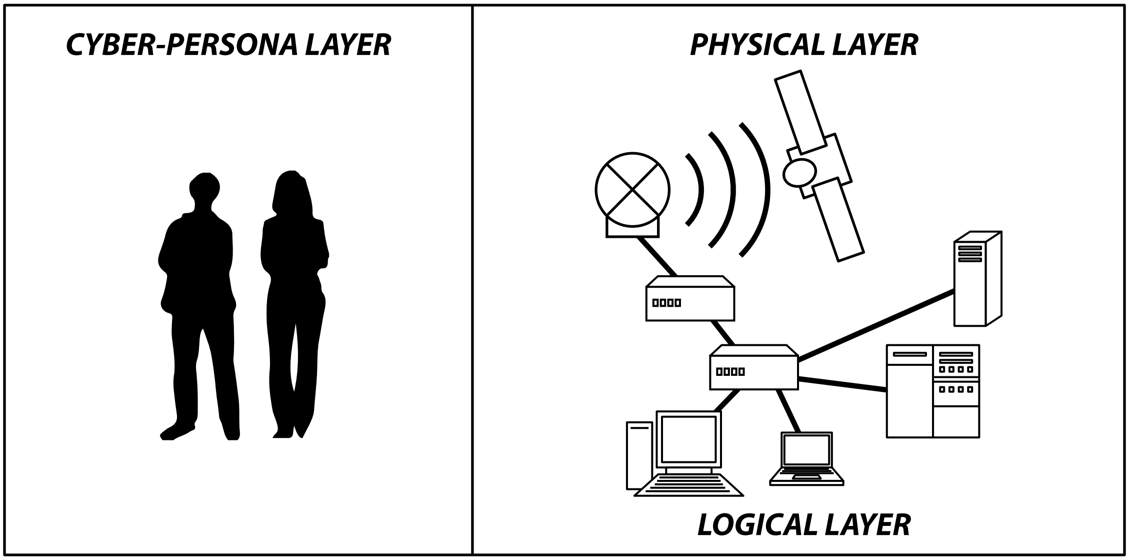

Figure 2. Cyber layers in space operations

The Exponential Domain

> *But if you think you're safe in cyber, when you wake up tomorrow, everything is different.*
>
> —Gen John E. Hyten, Commander
> Air Force Space Command

Ever since Intel cofounder Mr. Gordon Moore observed in 1965 that the capability of computer circuitry grows exponentially over time, it has been widely understood that innovation in computer technology expands at a rate unmatched in human history.[8] Innovation begets innovation, and the changing nature of information technology poses unique challenges for military operators in the cyberspace domain compared to those of the first four war-fighting domains.[9]

First among those challenges is that the private sector has now begun to advance far more rapidly than the defense industry in several areas of technological innovation.[10] This can mostly be attributed to the molasses-like procurement and configuration management processes in the Department of Defense's large technological programs relative to the nimbleness of a Silicon Valley start-up company.[11]

A second serious challenge is that the asymmetry of cyberspace allows attackers to more quickly and more easily utilize rapid changes to their advantage than can defenders.[12] At a fundamental level, cyber defenders attempt to ensure that software and hardware work the way they are supposed to while cyber attackers attempt to break software or hardware to cause harmful effects.[13] In this matchup, the aggressor will almost always have the advantage. Additionally, the exponential nature of cyberspace causes institutional knowledge and individual skill sets to atrophy far more quickly than they do in the traditional war-fighting domains. This poses especially interesting challenges for the training and education of cyberspace operators.

For all of its difficulties, the US Air Force has a well-established grasp on the current cyberspace battleground. Yet, it must fully account for the nature of cyber dependency and the implications it holds for the expanding cyber battleground of the future.

Self-Induced Dependency

> *The F-35 Lightning II is one of the most complicated weapons systems ever developed, a sleek and stealthy fighter jet years in the making that is often called a flying computer because of its more than 8 million lines of code.*
>
> —Christian Davenport, *Washington Post*

While the space domain is the first to be wholly dependent upon cyber, it will not remain the only one. In the air domain, remotely piloted aircraft are an excellent example of a weapon system that is wholly cyber dependent.[14] Even the newest manned fighter aircraft, the F-35, has been described as a flying computer; furthermore, while the Army develops personal drones, smart exoskeletons, and computerized rifles, the Defense Advanced Research Projects Agency is developing pack-mule robots, and the Navy is creating its own autonomous drones, including both submarines and aircraft.[15]

While those efforts will certainly enhance war-fighting capabilities, increased cyber dependency also comes at a cost. The cost may be paid in increased risk to the missions that these technologies support or in deliberate security and active defense of the newly dependent systems.[16] In each example, the inherent risks introduced by cyber dependency are monumental. In the civilian world, hackers have already been able to take control of vehicles (most notably gaining full remote control of the latest Jeep models), smart guns, and hobby drones. They have even infiltrated the internal networks of commercial aircraft.[17] For the cyber squadron of the future, security and defense of local weapon systems—from land and air to space—must be a priority (fig. 3).

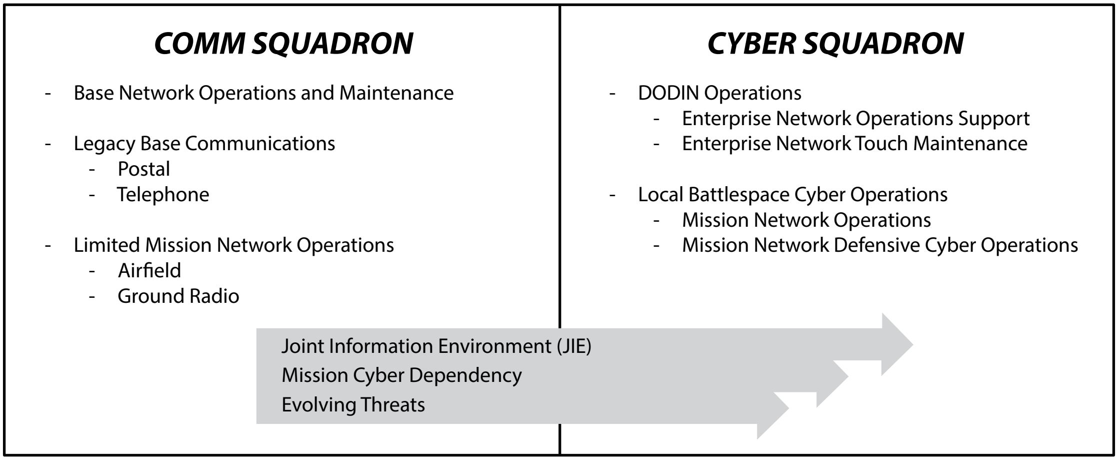
COMM SQUADRON
- Base Network Operations and Maintenance
- Legacy Base Communications
- Postal
- Telephone
- Limited Mission Network Operations
- Airfield
- Ground Radio
CYBER SQUADRON
- DODIN Operations
- Enterprise Network Operations Support
- Enterprise Network Touch Maintenance
- Local Battlespace Cyber Operations
- Mission Network Operations
- Mission Network Defensive Cyber Operations
Joint Information Environment (JIE)
Mission Cyber Dependency
Evolving Threats

Figure 3. From communications to cyber. (Based in part on briefing, Lt Col David Canady, subject: Cyber Squadron of the Future, Headquarters US Air Force / A6CF, May 2014, http://www.safcioa6.af.mil/shared/media/document/AFD-140512-040.pdf.)

One particularly thorny challenge for those cyber operators will be the requirement to perform cyber operations on the live network of a weapon system, but this challenge can and must be overcome.[18] Choosing not to secure and defend is the riskiest choice of all. In cyberspace, the longer any vulnerability exists in an unmitigated form, the greater the odds that it will be weaponized and exploited by an adversary. By some measures the process, from discovery to weaponization and attack, takes hackers little more than one week to complete.[19]

Cybersecurity concerns have not yet stopped the Department of Defense from procuring weapons that are increasingly cyber dependent. In the civilian world, regular consumers also seem to not yet be dissuaded by security concerns.

Market-Driven Cyber Dependency

> *These characteristics and conditions present a paradox within cyberspace: the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular.*
>
> —Joint Publication 3-12 (R),
> *Cyberspace Operations*, 5 February 2013

Market forces in the civilian world are rapidly driving many categories of consumer products towards the "Internet of Things" (IoT). By 2020 it is estimated that there will be between 50 and 100 billion devices that are networked to each other across the world, creating an IoT.[20]

From refrigerators to coffeepots and thermostats, the commercial marketplace is growing increasingly flooded with Internet-aware devices of all types.[21] Arguably, the preponderance of devices in the marketplace in the near future will be Internet-aware, making it difficult for a discerning consumer such as the Department of Defense to find noncomputerized alternatives.[22] This will leave the military with difficult choices to make regarding the trade-off between accepting risk or accepting the costs associated with cybersecurity and defense of these newly networked refrigerators and coffeepots.

If we accept that in the future a much higher percentage of devices, infrastructure, and systems will have computer networking capabilities that are either a permanent part of military installations (such as supervisory control and data acquisition [SCADA]) or will regularly enter military installations (such as smart watches and self-driving cars), then those devices will become a de facto part of the cyber battlespace. It is the cyber squadron of the future that should be relied upon to secure and defend those devices. Efficiencies provided by organizational and structural changes such as the move to the joint information environment, as well as new technologies such as software-defined networking, may free up many of the resources required to allow the cyber squadron of the future to secure and defend the expanded cyber terrain; however, additional investment and reforms will also be needed to sustain these new requirements.[23]

Winning Tomorrow's Fight

Given the speedy movement towards greater cyber dependency throughout the military, it is critical that Air Force Space Command examine and consider the following recommendations for the cyber and space force-development systems.[24]

Leverage Big Data for Decision Making

Air Force Space Command should develop three standard tests and should implement them throughout the force-development process to assess both space and cyber Airmen. The first test should be for cyber proficiency and propensity only. This test would measure a recruit's or trainee's potential to comprehend cyber concepts and acquire cyber skills, regardless of formal cyber training.[25] The second and third tests would be knowledge based—one for knowledge applicable to cyberspace operations and the other applicable to space. Initially, it may be impossible to determine exactly what cyber proficiency looks like. This is acceptable and should not dissuade the command from undertaking this effort. As scores for all three tests are compiled, they must be associated with members and tracked alongside other metrics to determine how scores appear to correlate to a given individual's success, mediocrity, or failure. The process of data compilation and analysis should continually in-form a cyclical reevaluation of the tests to ensure that they adequately assess ability and knowledge.

Pertinent data points that should be associated with test scores fall into three major categories: education, training, and experience. By combining proficiency and knowledge test scores with data points from these three categories, Air Force Space Command will gain powerful insight into how to prioritize education, training, and experience when it makes force-development decisions. By strategically retesting Airmen, the command can gain insight into how specific training events or educational milestones affect or do not affect scores.[26]

Mission-Specific Cyber Training

Air Force Space Command is close to having implemented the optimal framework for an initial, intermediate, and advanced training system for cyberspace operations. The current focus on mission-specific intermediate training as opposed to general intermediate training and on-the-job training is a great leap in the right direction.[27] Increased cyber dependencies will create the need for many additional mission-specific training courses such as SCADA and IoT defensive operations, as well as intermediate cyber defensive training that is specific to various Air Force land, space, and air mission systems.

For enlisted Airmen, the 1B initial training course should be split between a combined 3D and 1B initial training course and intermediate training courses that are specific to the mission requirements that 1B and 3D Airmen will encounter. The 3D career fields should not be left out of the operationalization of the communications career fields because they play important roles in the security and defense of the cyber battleground and will continue to do so. Efforts to divide training requirements between the 3D and 1B career fields should follow the National Institute of Standards and Technology's National Initiative for Cybersecurity Education Framework.[28] While training for enlisted 3D and 1B Airmen will diverge fairly quickly after the basics, there must be a set of core "operational cyber" fundamentals shared by the two career tracks.[29]

Specialized Training for Cyber-Dependent Operators

For those noncyber officers whose mission sets have high levels of cyber dependency, such as space operations personnel and remotely piloted aircraft pilots, opportunities should be made available for them to attend the intermediate and advanced cyber training that is applicable to their mission. Program acceptance for noncyber Airmen should be based in part on their cyber proficiency and knowledge test scores.

Just as there is an advantage provided by having weapons officers who are proficient across the spectrum of weapon systems, so would it be advantageous to have officers in cyber-dependent missions who are also proficient in cyber operations.[30] A program similar in many ways to the one offered by the USAF Weapons School but with a smaller footprint should be established to strategically place graduates within their cyber-dependent career fields.[31]

Work to Expand Industry Partnership Opportunities

Air Force Space Command should work with the Office of the Assistant Secretary of the Air Force for Acquisition (SAF/AQ) and the Air Force Institute of Technology (AFIT) to create a special pipeline for officer and enlisted Airmen in the space and cyber career fields to tour in the Education with Industry (EWI) program. If this cannot be accomplished, Air Force Space Command should consider establishing a similar program, focused on bringing cutting-edge innovation and specialized skills back to the military while expanding ties with industry partners.

Graduates of the EWI program not only help close the technology and skills gap between the military and the private sector but also help increase cooperation and strengthen ties between the two sectors at a critical time for space and cyberspace.[32] Air Force Space Command should focus on embedding officer and enlisted Airmen within corporations that are at the forefront of space and cyberspace technology and should press to expand outside the list of traditional cleared defense contractors.

Though the EWI program is not generally made available to enlisted Airmen, space and cyberspace require unique technical skills that can be developed and grown during an EWI tour. While an officer in the EWI program may develop unique leadership skills and pick up innovative ideas, correctly placed enlisted Airmen could bolster their coding or other technical skills that are specific to their mission and career field.

These efforts would be in line with Secretary of Defense Ashton Carter's initiative to increase innovation in the Department of Defense and strengthen military and industry ties.[33] In addition to coordination with SAF/AQ and AFIT on the EWI program, Air Force Space Command should seek to develop direct ties with Defense Innovation Unit X, the new Department of Defense cell in Silicon Valley.[34] Because Unit X will primarily develop and strengthen industry ties in the area of cyber operations, Air Force Space Command would benefit from coordinating with Unit X on force development of cyberspace operators.[35]

Encourage New Forms of Education and Training

The civilian market for Internet-based microdegrees, nanodegrees, and other forms of short-term, topic-specific training has greatly increased cost-effective education and training opportunities for Airmen to leverage.[36] Shorter than an associate degree but longer than a traditional training course, microdegrees and other new forms of Internet-based learning have proliferated in recent years. Air Force Space Command should actively embrace and explore this trend as a way to train and educate space and cyber Airmen. Partnerships with online learning companies such as Udacity, Coursera, edX, or other massive open online course (MOOC) providers may yield opportunities for Airmen to gain topical education and training customized to the needs of Air Force Space Command, with much lower entry costs and time barriers for students.[37]

Traditional education still has a very important role to play, but Air Force Space Command should take active steps to investigate how these education technologies are changing the civilian education market.[38] Microdegrees can provide Airmen with a far more agile, topical, and responsive form of education that also allows them to stay up to date in the rapidly advancing field of information technology. Beyond individualized education and training, partnerships between Air Force Space Command and MOOC companies could provide a relatively cost-efficient way to train space and cyber Airmen on the whole.[39]

Extensive Investment in the Cyber Training Corps

Of all the war-fighting domains, cyber's exponentially changing terrain makes "teaching cyber" a challenging task over time. Comparatively, very little changes year-to-year as pilots are trained in air operations or as space operators are trained in space operations, yet course material in the cyber domain may become outdated within months.[40]

Just as an individual operator's skills and knowledge will atrophy far more rapidly than in the other domains, so will material developed for training and education.[41] For every instructor assigned to a cyber instructional course, Air Force Space Command should consider assigning a second member whose responsibilities include rapid revision of course material based on changing circumstances in the cyber domain and tuning based on analysis of student feedback and performance.

While the instructor handles instruction, grading, and administration, a course developer would be tasked to ensure that course instruction remains timely and relevant. Whenever possible, course developers should be embedded with operational units and/or industry partners in the private sector for short bursts of time to retain cutting-edge knowledge and skills.[42] Like an information system with known vulnerabilities, cyber instructional courses cannot afford to remain static; instead, they must be treated like a constantly evolving system. For every cadre of instructors, there should be an equally large or greater cadre of course developers handling this function.

Conclusion

Of all the war-fighting domains, cyberspace is the most rapidly changing. These changes are driving Air Force missions and weapon systems towards greater cyberspace and space dependency. By understanding, anticipating, and posturing for greater degrees of cyber dependency throughout the force, Air Force Space Command will develop space and cyber Airmen who are ready to prevail in the cyber battleground of the future.

Air Force Space Command should consider the advantages of leveraging big data for decision making, continuing to develop mission-specific cyber training, making cyber training available to operators in cyber-dependent missions, strengthening ties with industry partners, encouraging new forms of education and training, and investing heavily in an expanded cyberspace training cadre. These investments, some small and some large, would yield sizable dividends when Air Force Space Command suddenly finds itself immersed in the cyber battleground of the future. It is possible to imagine, at some near-distant point in the future, an Air Force that is wholly dependent on space and cyberspace. It is equally possible to envision an Air Force whose cyber defense capabilities are far greater than the new threats that these space and cyber dependencies will pose. The time to begin overcoming the challenges of cyber dependency is now. ✪

Notes

[1] Degrees of cyber dependency may be used to describe any military capability, technology, or strategy. Supremacy in the cyberspace domain is analogous to air supremacy and is defined by the author as the degree of cyber superiority over a portion or segment of cyberspace wherein the opposing cyber force is incapable of effective interference.

[2] Market forces will drive the military to secure and defend a larger battlespace, but the Department of Defense itself will also deliberately expand the cyber battlespace in a much more consequential way.

[3] Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, 5 February 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. JP 3-12 refers to this as the "[unique] relationship" between space and cyberspace. The author calls this "domain cyber dependency" because all operations in the space domain presently rely on cyberspace supremacy.

[4] Ibid.; and JP 3-14, *Space Operations*, 29 May 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

[5] JP 3-12 (R), *Cyberspace Operations*, defines cyberspace as "many different and often overlapping networks, as well as the nodes (any device or logical location with an internet protocol [IP] address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them" (I-2).

[6] Ibid.

[7] Ibid. With regard to space operations, the physical network layer of cyberspace includes the information systems with which space operators perform command and control operations and receive and analyze telemetry; the circuits connecting those information systems to the ground equipment; the ground equipment itself, which prepares and sends data to the space vehicle; and the space vehicles themselves. The logical network layer of cyberspace is embedded in each piece of the physical network. When space operators change configurations on or send commands to any part of the physical network layer, encrypt or decrypt transmissions, or perform data aggregation and analysis, they are operating within the logical network layer of cyberspace. To some degree, these actions may be considered cyberspace operations. The cyber-persona layer describes the space operators who rely on the physical and logical network layers to perform space operations. The cyber-persona layer also includes potential adversaries who may disrupt space operations through their own cyberspace operations.

[8] Damon Poeter, "How Moore's Law Changed History (and Your Smartphone)," *PC*, 19 April 2015, http://www.pcmag.com/article2/0,2817,2482133,00.asp.

[9] JP 3-12 (R), *Cyberspace Operations*; and Mark Pomerleau, "Army Cyber Chief Outlines Key Challenges, Goals," Defense Systems, 18 March 2015, http://defensesystems.com/Articles/2015/03/18/Army-cyber-Cardon-outlines-challenges-goals.aspx.

[10] Max Boot, "The Paradox of Military Technology," *New Atlantis*, no. 14 (Fall 2006): 13–32.

[11] Jose Pagliery, "Love, Not War: Pentagon Courts Silicon Valley," *CNN*, 23 April 2015, http://money.cnn.com/2015/04/23/technology/security/military-silicon-valley/.

[12] Lt Col Gregory Conti and Col John "Buck" Surdu, "Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?," *IAnewsletter* 12, no. 1 (Spring 2009): 14–18; and Andrew Phillips, "The Asymmetric Nature of Cyber Warfare," US Naval Institute, 14 October 2012, http://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare.

[13] JP 3-12 (R), *Cyberspace Operations*.

[14] Katia Moskvitch, "Are Drones the Next Target for Hackers?," BBC, 6 February 2014, http://www.bbc.com/future/story/20140206-can-drones-be-hacked; and Aliya Sternstein, "How to Hack a Military Drone," DefenseOne, 29 April 2015, http://www.defenseone.com/technology/2015/04/how-hack-military-drone/111391/.

[15] Christian Davenport, "Meet the Most Fascinating Part of the F-35: The $400,000 Helmet," *Washington Post*, 1 April 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/04/01/meet-the-most-fascinating-part-of-the-f-35-the-400000-helmet/; "Insects Inspire Military Mini Drones," *Fox News*,

18 September 2014, http://www.foxnews.com/tech/2014/09/18/insects-inspire-military-mini-drones/; Joyce P. Brayboy, "Army Researcher's Interest in Robots Leads to Innovative Device," US Army, 2 July 2015, http://www.army.mil/article/151527; Terri Moon Cronk, "Robot to Serve as Future Military's 'Pack Mule,' " US Department of Defense, 19 December 2012, http://archive.defense.gov/news/newsarticle.aspx?ID=118838; Brendan McGarry, "U.S. Military Begins Testing 'Smart' Rifles," DefenseTech, 15 January 2014, http://defensetech.org/2014/01/15/u-s-military-begins-testing-smart-rifles/; and Kris Osborn, "Navy to Deploy First Underwater Drones from Submarines," Military.com, 13 April 2015, http://www.military.com/daily-news/2015/04/13/navy-to-deploy-first-underwater-drones-from-submarines.html.

16. Cybersecurity is most commonly understood to be compliance related, such as the management of vulnerabilities and the implementation of protective measures. This contrasts with active defense, which is the implementation of defensive measures or maneuvers in anticipation of, during, or after a cyber incident or engagement with an adversary.

17. "The Pentagon Got Hacked While You Were at Def Con," *Wired*, 9 August 2015, http://www.wired.com/2015/08/security-news-week-pentagon-got-hacked-def-con/; Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *Wired*, 21 July 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Kim Zetter, "Is It Possible for Passengers to Hack Commercial Aircraft?," *Wired*, 26 May 2015, http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/; and Hallie Golden, "Security Experts Point to OPM's Biggest Cybersecurity Failure," NextGov, 21 July 2015, http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-failure/118274/. In each of these examples, the exploits were uncovered by security researchers, not professional "militarized" hackers. If a well-organized, advanced, persistent threat were to commit its resources to similar targets, the results would likely be far severer.

18. JP 3-12 (R), *Cyberspace Operations*. Traditionally, the bulk of defendable battlespace in the cyberspace domain has been communications infrastructure that provides support to the primary mission. One implication of greater cyber dependency will be that the defendable battlespace will expand to include the mission systems themselves. The challenge posed is that intuitively, friendly disruption to the mission would be more likely while defensively operating on a mission or weapon system than it would be while defending communications infrastructure.

19. Recorded Future Special Intelligence Desk, "Week to Weak: The Weaponization of Cyber Vulnerabilities," Ref ID: 2014-02 (Somerville, MA: Recorded Future, 4 December 2014), http://go.recordedfuture.com/week-to-weak-report. The "Week to Weak" report, published in late 2014, illustrates the rapid speed at which vulnerabilities are now weaponized and seen in the wild. Analysis by Recorded Future found that the median number of days for a vulnerability to be exploited is only 7.5. For reference, the report cites the National Institute of Standards and Technology (NIST) as publishing roughly 7,000 newly known vulnerabilities in 2014. This illustrates the incredible speed at which cybersecurity measures such as vulnerability management must occur to maintain risk at appropriate levels.

20. "Standards Are Making the Internet of Things Come Alive," IEEE Standards Association, 8 April 2013, http://standardsinsight.com/ieee_company_detail/standards_iot; and Dr. W. Charlton Adams Jr., "The Internet of Things and the Connected Person," *Wired*, December 2014, http://www.wired.com/insights/2014/12/iot-connected-person/.

21. Klint Finley, "Hacked Fridges Aren't the Internet of Things' Biggest Worry," *Wired*, 12 March 2015, http://www.wired.com/2015/03/hacked-fridges-arent-internet-things-biggest-worry/; Bill Wasik, "In the Programmable World, All Our Objects Will Act as One," *Wired*, 14 May 2013, http://www.wired.com/2013/05/internet-of-things-2/; and Dan Saffer, "The Wonderful Possibilities of Connecting Your Fridge to the Internet," *Wired*, 29 October 2014, http://www.wired.com/2014/10/is-your-refrigerator-running/.

22. If the public is not dissuaded by privacy and security concerns, consumer preference for smart devices from self-driving cars to networked refrigerators should provide supplying firms a competitive advantage. If this is the case, competitors to those "first-mover" firms may seek to adopt the same technology or develop their own, potentially commoditizing the technology itself and driving out non-adopting alternatives from the market.

23. Cade Metz, "Mavericks Invent Future Internet Where Cisco Is Meaningless," *Wired*, 16 April 2012, http://www.wired.com/2012/04/nicira/; and Klint Finley, "GE's New Cloud Must Be the Most Tempting Hacker Bait Ever," *Wired*, 5 August 15, http://www.wired.com/2015/08/ges-new-cloud-may-tempting-hacker-bait-ever/.

24. Since space operations are overwhelmingly reliant on cyberspace supremacy, several but not all of these recommendations are cyber-centric.

25. A cyber proficiency test would likely assess logic-based problem solving as well as abstract thinking, two skills required for success in cyberspace (and in space).

26. Critically, these tests should not be used to affect the career vectoring of individuals during the first several years of implementation. Over time, as the tests are refined and conclusions are able to be teased out of data points, they will become useful in making those decisions. Drawing conclusions too quickly and making vectoring decisions during the refinement process would skew the results and only lead to foregone conclusions rather than provide true insight.

27. Capt Kinder Blacke, "Intermediate Network Warfare Training Up and Running," Air Force Space Command, 3 March 2011, http://www.afspc.af.mil/news/story.asp?id=123245023; and SSgt Jarrod Chavana, "Airmen Train for 'New Wild, Wild West' in Cyber Domain," *Santa Maria Times*, 10 October 2014, http://santamariatimes.com/news/local/military/airmen-train-for-new-wild-wild-west-in-cyber-domain/article_1633ec02-eb22-54e5-ad04-f4bea53b776c.html.

28. "National Cybersecurity Workforce Framework," National Initiative for Cybersecurity Education, accessed 15 October 2015, http://csrc.nist.gov/nice/framework/.

29. In addition to being informed by the NIST standards, initial and intermediate training for enlisted Airmen should be informed by operational techniques used in the joint community, such as the plan, brief, execute, debrief (PBED) process.

30. J. R. Wilson, "Interview: Col. Robert 'Shark' Garland, Commandant, USAF Weapons School," Defense Media Network, 6 November 2011, http://www.defensemedianetwork.com/stories/interview-col-robert-%E2%80%9Cshark%E2%80%9D-garland-commandant-usaf-weapons-school/.

31. Entry into the program and placement following the program could be managed very similarly to the procedures of the USAF Weapons School, without the need to develop an entire training program that is separate from the traditional intermediate and advanced cyber courses that are specific to the graduate's mission.

32. Jim Garamone, "Winnefeld: DoD Must Strengthen Public, Private Ties," US Department of Defense, 14 May 2015, http://www.defense.gov/news/newsarticle.aspx?id=128810; and Kevin Gilmartin, "Education with Industry Program Offers Different Perspective," Air Force Print News, 14 March 2008, http://www.hanscom.af.mil/news/story_print.asp?id=123090306.

33. Cheryl Pellerin, "Carter Seeks Tech-Sector Partnerships for Innovation," US Department of Defense, 23 April 2015, http://www.defense.gov/news/newsarticle.aspx?id=128655.

34. Mark Pomerleau, "Carter Details DoD's Innovation Plans," Defense Systems, 6 May 2015, https://defensesystems.com/articles/2015/05/06/carter-dod-innovation-plans-congress.aspx; and Patrick Tucker, "Pentagon Sets Up a Silicon Valley Outpost," Defense One, 23 April 2015, http://www.defenseone.com/technology/2015/04/pentagon-sets-silicon-valley-outpost/110845/.

35. Pomerleau, "Carter Details DoD's Innovation Plans."

36. Stuart M. Butler, "How Google and Coursera May Upend the Traditional College Degree," Brookings Institution, 23 February 2015, http://www.brookings.edu/blogs/techtank/posts/2015/02/23-mooc-google-coursera-butler/.

37. Ibid.

38. In addition to partnering with the companies themselves, an examination of the underlying technology and methods may illustrate efficiencies that could be implemented in military-led training courses.

39. Jeffrey R. Young, "Will MOOCs Change the Way Professors Handle the Classroom?," *Chronicle of Higher Education*, 7 November 2013, http://chronicle.com/article/Will-MOOCs-Change-Campus/142869/.

40. Conti and Surdu, "Army, Navy, Air Force, and Cyber," 14–18.

41. Ibid.

42. Semiregularly, instructors and course developers should rotate between their respective functions to retain currency in each.

2nd Lt Chris Babcock, USAF

Lieutenant Babcock (BS, Indiana University) is the crew commander and deputy section chief for the 50th Space Communications Squadron's Air Force Satellite Control Network, Network Operations Security Center. He is a cyberspace operations officer with a special interest in network defense and intelligence integration.

Let us know what you think! Leave a comment!

http://www.airpower.au.af.mil